A SECURE, OPEN AND INTEROPERABLE E-ORDERING SERVICE

Despina Polemi, Spyridon Papastergiou
Department of Informatics, University of Pireaus, 80 Karaoli & Dimitriou Str., Pireaus, Greece

Keywords: e-Ordering, XML, Web Services, Security, XML, Advanced e-signatures.

Abstract: Electronic Ordering (e-Ordering) services are fundamental in the provision of electronic trade. The contemporary e-Ordering implementations vary in terms of the underlined technologies, creating important interoperability and security problems. In this paper we capture the security requirements of the e-Ordering service and we present an e-ordering system based on the eXtensible Markup Language (XML), XML Cryptography, Public Key Infrastructure (PKI) and Web Services. Our proposed e-Ordering service is an open, secure and interoperable solution, respecting the EU legislation.

1 INTRODUCTION[1]

One of the most important transactions amongst commercial partners is the electronic ordering. The ordered documents may contain business data (e.g. VAT code, items) or private data that should not be revealed or modified. They should be trustful documents requiring all four dimensions of security (confidentiality, integrity, authenticity, non repudiation). The order service as a process should allow the true business-to-business secure collaboration by giving the opportunity to salesmen and purchasers to execute trustful processes of electronic trading opening new markets.

The advantages that e-ordering offers include: the generation of more revenue, improvement of sales efficiency, increase of customer retention, accuracy and efficiency of sales, elimination of costs (Microsoft, 2003).

The purpose of this paper is the presentation of the security and interoperability requirements of an e-ordering service, as well as the proposition of an open, affordable and scalable e-ordering architecture that satisfy these requirements complied with EU regulations and directives. The proposed system, in order to meet these objectives, is built using open technologies, such as eXtensible Markup Language (XML), XML Cryptography, Public Key Infrastructure (PKI) and Web Services.

The rest of this paper is organized as follows. Section 2 provides the fundamental security requirements of e-ordering. Section 3 describes in detail the e-ordering system architecture and its components. Finally Section 4 presents our conclusions and areas for further research.

2 STATE-OF-THE ART AND REQUIREMENTS

In this section we present the e-Ordering security requirements as well as technical countermeasures that address these requirements.

2.1 Security Requirements and Measures

The e-Ordering systems have to satisfy certain fundamental security requirements:

Authentication of origin. The confirmation of the source that sends the orders is a critical issue of the ordering exchange process. This requirement can be addressed using XML digital signatures in combination with tamper resistant cryptographic modules such as smart cards.

Integrity of the content. During transmission or storage time, the orders should be protected from

[1] The research of the present paper has been supported by the eTen project SELIS (selis.unipi.gr) and by the GSRT(PENED) programmes.

Polemi D. and Papastergiou S. (2006).
A SECURE, OPEN AND INTEROPERABLE E-ORDERING SERVICE.
In *Proceedings of WEBIST 2006 - Second International Conference on Web Information Systems and Technologies - Internet Technology / Web Interface and Applications*, pages 57-62
DOI: 10.5220/0001252900570062

unauthorized (intentionally or accidentally) modification or their replacement. The use of a cryptographic hash function, that provides message integrity checks, can be achieved either separately or as part of the digital signature process.

Non-repudiation of origin and receipt. The ordering exchange can not been denied neither by the sender nor by the recipient. Digital signatures and time stamping (Sklavos et al, 2001) are the measures to address this requirement.

Long lasting integrity. The electronic signatures of the orders should remain valid over long periods. To face this problem, ETSI produced ETSI TS 101 903 (commonly known as ***X***ML ***Ad***vanced ***E***lectronic ***S***ignatures-XADES-) to define XML formats for advanced electronic signatures. A XAdES electronic signature offers also non-repudiation based on a predefined signature policy (XAdES, 2002).

Confidentiality and privacy. The orders should be readable by the designated recipients. This can be achieved using XML Encryption as specified in the W3C Recommendation (Eastlake, 2002) and the Web Services Security recommendation for encryption in SOAP messages (Nadalin, 2004), (Hartman, 2003).

Integrity of the sequence of the orders. This requirement translates in to the avoidance of missing orders. Addressing this requirement can be done with the imposition of a tight sequence issuance scheme by having a reference number embedded in each order.

Availability. The e-ordering service will be able to be used at any time from the enterprises. Because of this fact, serious security issues can arise and the system have to be protected against intrusion and hacking. Perimeter security (e.g. installation of Intrusion detection systems, antivirus and firewalls) can be used to meet these requirements. On the other hand, Web Services will have to provide published services in registries, in which any interested entity will have the opportunity to search and invoke a desirable service.

Secure Electronic Storage. Primary requirements, such as authenticity, integrity and readability should be guaranteed throughout the storage period of the e-ordering documents. An ideal system that can be used for this purpose is a native XML database. The essential result from the use of such type of system is the possibility of storage of XML orders with the original format in which they were received. Furthermore, the combination of XAdES and a native XML database can guarantee the secure long-term archiving of e-orders.

Legal Compliance. All e-ordering implementations have to be compliant to a set of regulations and directives that are defined from the legal framework of EU member states e.g. Digital Signature Law Privacy and Electronic Communication Regulations Electronic Commerce Directive Electronic Storage Directive.

3 A SECURE E-ORDERING SERVICE

In this section we will present our proposed e-Ordering service architecture, the entities that are involved in the service, the procedures and necessary steps that these entities have to follow in order to complete an e-Ordering transaction.

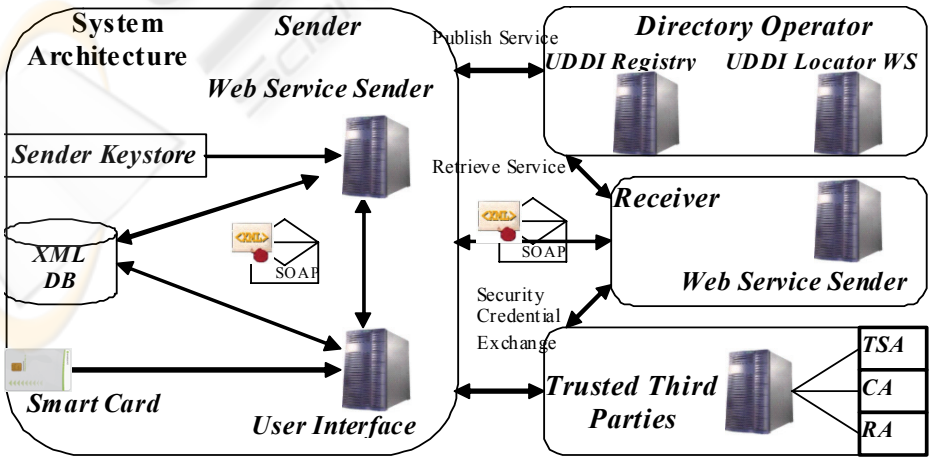

Figure 1: System Architecture.

3.1 Service Architecture

Our proposed system adopts the most advanced and widely adopted standards for secure interoperable service provision currently available. The system is addressing the requirements described in Section 2.1.

Technologies, such as XML and Web Services, are used to achieve security and interoperability. The message format integrated in the current version of the system uses the XML Common Business Library version 4.0 (xCBL 4.0) (xCBL.org, 2003), which is a set of XML building blocks and a document framework that allows the creation of robust, reusable, XML documents to facilitate global trading.

XML is used for formatting the e-order document, which allows the use of XML digital signatures and the integration of timestamping tokens to the document. The XML schema adopted for the e-order is a subset of xCBL. The selection of xCBL is based on its maturity level of completeness and clarity.

The exchange mechanism for e-orders relies on the Simple Object Access Protocol (SOAP) (Nadalin, 2004), (Harman, 2003) messaging with Web Services Security extensions. Storage is handled natively by an XML database to satisfy the requirement for secure storage of the exchanged e-orders in the form in which they were sent and received. Integrity and non-repudiation for the e-order documents is ensured by the use of XML digital signatures so that origin and integrity information are embedded in the e-order document (Kaliontzoglou, 2006).

Figure 1 depicts the three major components i.e. User Interface, Web Service Sender and XML Database of the system architecture. These components are described in details as follows:

a) ***User Interface***. The User Interface gives the possibility to the user to create, to manage and to send orders. In order to achieve this, it communicates with six entities:

User card, to sign the orders. **CA (Certification Authority)**, to request certificate status information (Kaliontzoglou, 2006). **TSA (Time Stamping Authority)** to request time stamps, in order to produce XAdES signature (Kaliontzoglou, 2006). **XML database**, to retrieve order's information. **Web Service Sender**, in which the orders are sent. **UDDI Registry**, to publish the e-Ordering Service.

b) ***Web Service Sender***. The Web Service Sender communicates with five entities:

User Interface, that sends the orders to the Web Service Sender. **XML Database**, to store orders and receipts. **Sender Keystore**, to receive sender certificate and receiver certificate. **Web Service Receiver**, which receives the orders. **UDDI Registry**, to retrieve the URL of the Web Service Receiver.

c) ***Native XML database***. The XML database (Meier., 2002) communicates with two entities:

User Interface, which retrieves orders' information. **Web Service Sender**, which stores orders and receipts.

In Addition, Figure 1 depicts the four major

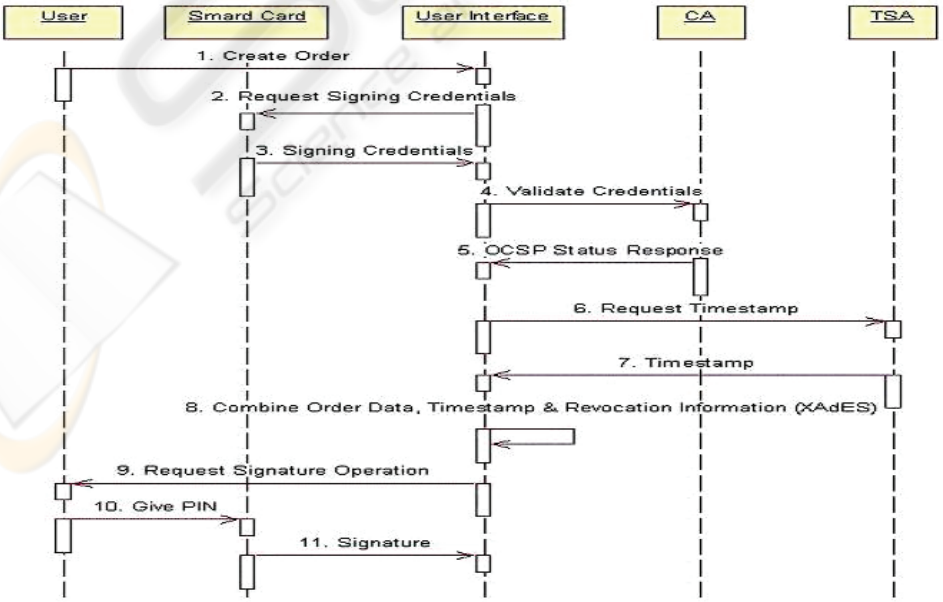

Figure 2: Sequence diagram for the e-Ordering process (Actions 1-11).

entities that take part in the e-Ordering process. The two major entities that participate to the transaction are the Sender that initiate the process and the Receiver that receives the order. A detail description of these entities is the following:

a) ***The Sender***. The Sender is an organization that hosts the system architecture as it is described above (Figure 1). The Sender deploys the e-Ordering service and publishes it in the UDDI Registry. It also communicates with the Trusted Third Parties to get the proper security credentials.

b) ***The Receiver***. The Receiver is an organization that hosts the above e-Ordering service architecture or a similar one. The fundamental requirement is that the architecture that the Receiver should adopt must be able to understand the xCBL order schema, and the SOAP messages with WS security extensions. Then, the Receiver retrieves the e-Ordering service from the UDDI and it is configured to understand the messages. It also communicates with the Trusted Third Parties to get the proper security credentials.

c) ***The Trusted Third Parties (TTPs)***. The TTPs that are required in the proposed architecture are a Certification Authority (CA) and a Registration Authority (RA) offering the PKI services of registration and certification (Adams, Lloyd, 1999)., and a Time Stamping Authority (TSA*)* offering standards based time stamping services (Sklavos et al, 2001).

d) ***Directory Operator***. The Directory Operator Entity is composed of the UDDI Registry, and UDDI Locator WS.

UDDI Registry is the directory where Web Services can be published. **UDDI Locator WS**, the use of this directory makes possible the discovery of the UDDI in which a Web Service has been published.

3.2 e-Ordering Processes

The Sender and the Receiver of the order, before, initiate the e-Ordering process, have to accomplish a set of actions, which are divided in two phases. The first phase constitutes the communication with the UDDI Registry for the publication and retrieval of the e-Ordering service. In the second phase the Sender and the Receiver have to communicate with the TTPs for acquisition of the security credentials.

Phase1: Service publication and retrieval. The

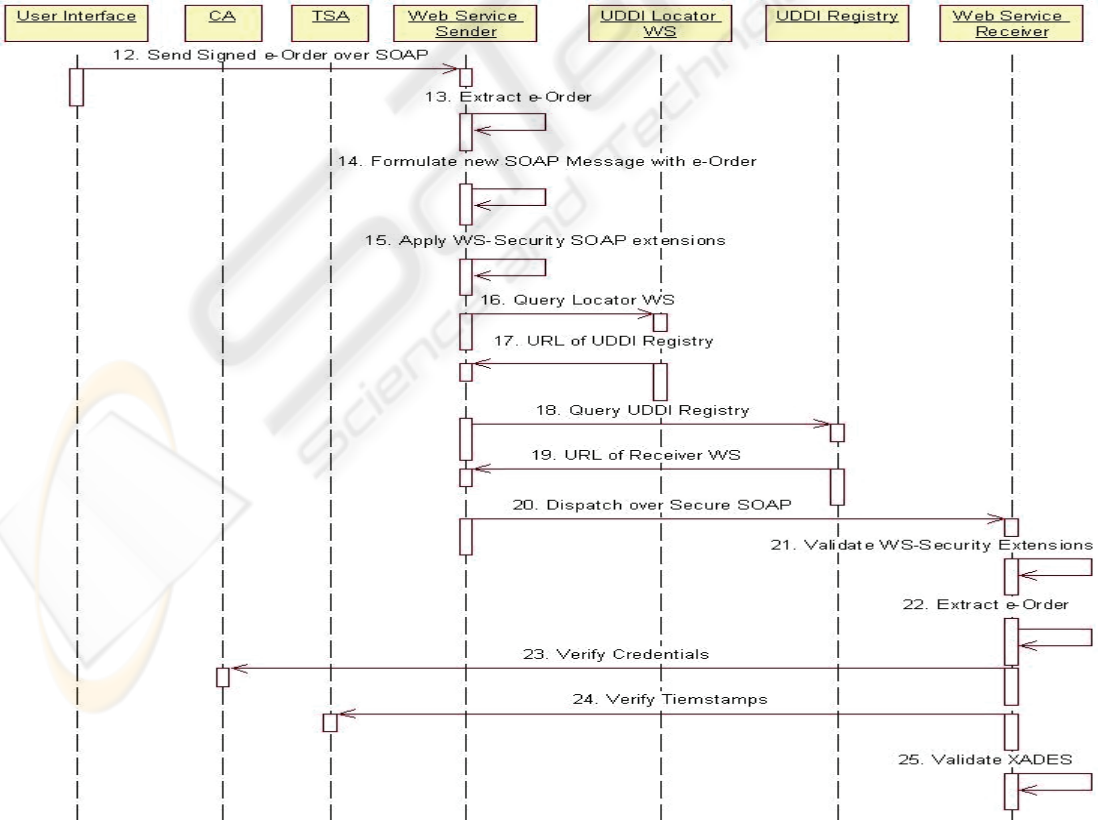

Figure 3: Sequence diagram for the e-Ordering process (Actions 12-25).

Sender produces the WSDL document and publishes the e-Ordering service to the UDDI Registry. Then the Receiver retrieves the description from the UDDI registry and configures its service to be able to receive and send SOAP message according to this description. Furthermore, the Receiver produces the WSDL document that corresponds to its service and publishes its service to the UDDI Registry.

Phase2: Set up security Credentials. The Sender and the Receiver take part in the Registration and Certification procedures as demanded by the Certification Practice Statement of the TTP, and setup the acquired security credentials, in order to achieve a secure communication. Moreover, they have to define the necessary signature policies that will be referenced while producing and validating XAdES signatures, as described in the XAdES standard (Kaliontzoglou, 2006).

When the Sender and the Receiver have accomplished the aforementioned phases, they are now ready to initiate the ordering process. The necessary steps to complete this process are illustrated below:

Step1: Access User Interface and Create Order Document (Action 1 (Figure2))

The e-Ordering process is initiated by an employee of an organization which wants to make an order. The user access a User Interface using a browser. The User Interface enables user to complete the necessary data in order to create an order or to manage existing orders. The data input is automatically checked for prevention of errors and is used to create the order document.

Step2: Sign Order Document (Actions 2-11 (Figure2))

When the order document has been created, the User Interface transparently gathers the time stamps and revocation status information data from their respective sources. Then, the XAdES signature is formulated based on the cryptographic primitives in the smart card, the user's certificate and the order data. At the end, the order document is signed using the qualified certificate of the user, which is located in the smart card.

Step3: Dispatching Signed Order Document to Sender's Web Service (Actions 12-19 (Figure3))

After the successful creation of the signed order document, the order document is packaged in a SOAP message and is dispatched to the Sender's Web Service. The Sender's Web Service extracts the order and packages it in a new SOAP message. WS Security extensions are applied to the new SOAP message. Then the new SOAP message is encrypted with the Receiver's public key, and is digitally signed with the Sender's server private key. The Sender's Web Service queries the UDDI Locator WS in which UDDI Registry the Receiver has published its Web Service. The query is based on the VAT prefix of the Receiver that corresponds to the country code. When the Sender's Web Service receives the UDDI Registry URL, it queries the Registry in order to receive WSDL document. Then the WSDL document is parsed and Sender's WS retrieves the URL of Receiver's Web Service.

Step4: Receipt of Order at Receiver's Web Service (Actions 20-25 (Figure3))

The protected SOAP message, that has been created, is dispatched over HTTP to the Receiver's Web Service. The Receiver's Web Service receives the order and follows a fully automated process that requires no human intervention. The SOAP message containing the orders are decrypted with the Receiver server's private key and the validity of their WS Security extensions digital signature is verified, so that the point of origin is validated.

Then the e-Order document itself is extracted. Validation of the embedded cryptographic information firstly requires communication with a CA for verification of the credentials that were used to sign the e-Order as well as verification of any

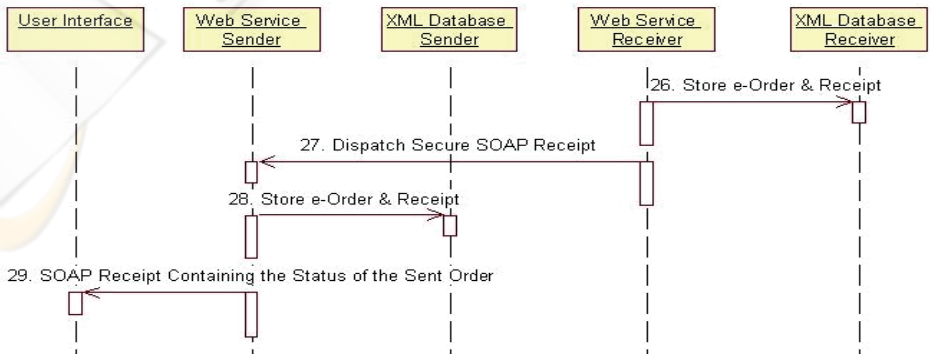

Figure 4: Sequence diagram for the e-Ordering process (Actions 26-29).

timestamp that was included in the document. Finally the XAdES signature is validated.

Step5: Storage of Order at Receiver's XML Database and Dispatching a Receipt (Actions 26-27 (Figure4))

The Receiver's Web Service stores the e-Order and a receipt in the Receiver's XML Database. From now on, the e-order is available for parsing and further processing by the Receiver's users. Then, the Receiver's Web Service dispatches the SOAP receipt, referencing to the received order, and containing the status of the whole process. The SOAP receipt is signed by the receiver's server in order to be valid as a receipt.

Step6: Storage of Order at Sender's XML Database (Actions 28-29 (Figure 4))

The Sender's Web Service receives the signed SOAP receipt and it stores it in its XML database along with the sent order.

4 CONCLUSIONS AND FURTHER RESEARCH

In this paper, we presented an architecture for a secure e-Ordering service. The proposed system is a secure tool for SMEs which desire to send and receive electronic orders via the Internet in a trustful manner. From a technological point of view, the system is compliant and in accordance with state-of-the-art standards that constitute an interoperable, affordable and scalable solution that address the security requirements, described in Section 2.1. The architecture is based on XML, XML digital signatures and encryption, xCBL and Web Services.

Our future research plan is to enhance the functionality and interoperability features of the proposed architecture addressing two more requirements: mobility and privacy. Our interest is focused on the implementation of the Privacy requirements as they are specified in the W3C working draft "Web Service Architecture (WSA) Requirements" (Austin, 2002) in the current electronic version of the service and in its future mobile version.

REFERENCES

Meier., W., 2002. eXist: An Open Source Native XML Database, In Lecture Notes In Computer Science, Revised Papers from the NODe 2002 Web and Database-Related Workshops on Web, Web-Services, and Database Systems, Springer-Verlag.

Adams, C., Lloyd, S.. 1999. Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations, Macmillan Technical Publishing, 1st Edition.

A. Kaliontzoglou, P. Boutsi, D. Polemi , 2006. "eInvoke: Secure e-Invoicing based on Web Services", Electronic Commerce Research, Kluwer, 2006 (to appear).

Sklavos et al, 2001. Time stamping in e-commerce, *E-Business E-work EBEW 2001 proceedings*, IOS Press.

Austin, D., 2002. Web Services Architecture Requirements, Internet draft, work in progress.

Microsoft, 2003. eOrder, Business Solutions-Great Plains.

XAdES, 2002. ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES).

Eastlake, D., Reagle, J., 2002. XML Encryption Syntax and Processing, W3C Recommendation, www.w3.org/TR/xmlenc-core.

Nadalin, A., 2004. Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard, docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

Hartman, B., 2003. *Mastering Web Services Security*, Wiley Publishing.

Message Authentication Codes (MAC), 2002, Cryptographic Message Syntax (CMS) Algorithms, IETF RFC 3370.

Secure Sockets Layer (SSL) http://wp.netscape.com/eng/ssl3/.

xCBL.org, 2003, XML Common Business Library version 4.00 (xCBL v4.00). www.xcbl.org/xcbl40/xcbl40.html.

European Parliament, 1997. "Privacy Act in the Telecom Sector, Directive 97/66/EC"

European Parliament, 1995. "Free movement, Directive 95/46/EC"

European Parliament, 1996. "Legal protection of databases, Directive 96/9/EC".

Directive 1999/93/EC of the European Parliament on electronic signatures Official Journal L 013 , 19/01/2000 p. 0012 – 0020, http://europa.eu.int/ISPO/ecommerce/legal/digital.html

European Parliament, 2000. "E-commerce, Directive 2000/31/EC". http://europa.eu.int/ISPO/ecommerce/legal

European Parliament, 2002. "Protection of Privacy, Directive 2002/58/EC". http://europa.eu.int/ISPO/ecommerce/legal